SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

OSNOVE KORIŠTENJA KRIPTOVALUTA

Mentor:
Dr.sc. Marko Hell

Student:
Anita Marija Ćapin, br.indeksa 5160731

Split, rujan 2018

Sadržaj

1. UVOD

U svijetu gdje tehnologija preuzima sve veću ulogu, gdje je područje bez interneta nemoguće zamisliti, a dobar dio ljudi uslijed financijskih kriza izgubio povjerenje u financijske sustave javila se potreba za drugačijim pristupom u rješavanju poteškoća. Kriptovalute su donijele cijeli niz drugačijih postavki financijskog sustava koji je u mnogočemu različit od tradicionalnih novčanih oblika. Zadnjih nekoliko godina digitalni novac općenito, a posebno nove digitalne valute sve više postaju predmet interesa javnosti. Velika praktičnost i brzina obavljanja elektroničkih transakcija u odnosu na klasične, su čimbenici koji već sada nedvojbeno utječu na porast popularnosti različitih oblika elektroničkog plaćanja. Digitalne valute na ovom polju donose nove mogućnosti uporabe. U svijetu postoji cijeli niz primjera plaćanja kriptovalutama i razmjena cijelih poslovnih procesa putem istih. U Hrvatskoj postoji još određena skepsa prema njihovom korištenju te je mnogo manja mogućnost njihovog korištenja.

1.1. Predmet istraživanja i ciljevi rada

Glavni predmet istraživanja ovoga rada je definiranje pojma i primjeri kriptovaluta koji se se koriste u modernom poslovanju. Cilj rada je detaljno definiranje kriptovaluta sa informatičkog stajališta. U tom smislu će biti prikazani načni njihovog osmišljavanja i načina rada sa stajališta njihovog funkcioniranja kao sustava. Drugi cilj je definiranje i mogućnosti primjene kriptovaluta kao sredstva plaćanja.

1.2. Metode rada

Različite metode rada su korištene prilikom izrade ovog završnog rada. Za prikupljanje podataka korištena je metoda „za stolom“. Najveći broj informacija i podataka prikupljeno je sa interneta i međunarodno priznatih znanstvenih članaka iz stručne literature poput znanstvenih časopisa i zbornika radova. U kasnijem radu korištene su i deduktivna metoda, metoda sinteze i analize, metode klasifikacije i metode deskripcije kao i najčešće korištena metoda komparacije.

1.3. Struktura rada

U prvom dijelu ovoga rada dan je teoretski prikaz pojma i osnove kriptovaluta. Dan je prikaz osnovnih pojmova koji su bitni za razumijevanje funkcioniranja kriptovaluta, njihovog korištenja. Osim tehničkih aspekata samog programiranja i funkcioniranja, dan je i teoretski prikaz načina rada, mogućnostima dobavljanja i pohrane istih. Također su i dani prikazi nekih od najrelevantnijih svjetskih kriptovaluta sa kojima se u svijetu rade više milijunske transakcije svake godine. U drugom dijelu rada je dan prikaz operativnog funkcioniranja transakcija U tom dijelu su objašnjeni oblici digitalnog novca, načini njegovog pohranjivanja, kao i same transakcije, načini na koje se izvode. U trećem dijelu rada dan je kratki prikaz korištenja kriptovaluta u međunarodnom poslovanju kao i dostupni primjeri iz Hrvatske.

2. KRIPTOVALUTE- OSNOVNI POJMOVI I ZNAČAJ

2.1. Pojam kriptovaluta

Kriptovalute (eng. cryptocurrency) su valute utemeljene na kriptografiji. Kriptovalute su prvenstveno softver, tj. zapisi unutar programa koji je instaliran na više računala koja su međusobno umrežena. Kriptovaluta je u potpunosti digitalna valuta čije se korištenje temelji na povjerenju zasnovanom na kriptografiji. Svaki se financijski sustav temelji na povjerenju, pa tako i Bitcoin, no kod Bitcoina „povjerenje se ne stječe po sili zakona, regulative ili službenim dekretima, nego se zasniva na povjerenju u matematiku, odnosno kriptografiju“ [1]

Sustav izgradnje povjerenja i konsenzusa u osnovi je financijski sustav (makar rudimentaran), a digitalni zapis koji je okosnica takvog sustava može postati vrijednost, odnosno valuta, te bi se mogao koristiti kao novac Za razliku od fiat-valuta koje se bez privole, nužno moraju koristiti po sili zakona, uporaba Bitcoina i drugih kriptovaluta ostavlja se slobodnoj volji građana, te je stoga interesantno postupno prihvaćanje kod šireg kruga korisnika. Naime, privlačnost dizajna Bitcoin sustava kao cjeline temelji se na ukupnosti pojedinačnih temeljnih elemenata (počela) koji ga čine. Neki od ključnih elemenata koji kriptovalute čine tako zanimljivima su:

- hijerarhija bez središnjeg autoriteta,
- nepostojanje institucija,
- izbacivanje posrednika koji ne pružaju značajniju dodanu vrijednost,
- inflacija je nemoguća,
- količina novca je ograničena,
- svaka se transakcija javno registrira ali ne postoje personalni identifikatori,
- sustav počiva na ekonomskim poticajima sudionicima koji međusobno konkuriraju za nagradu u utrci za verifikaciju transakcija i rješenje kriptografskog problema.. [2]

2.2. Razvoj kriptovaluta

Osnovni čimbenici u funkciji razvoja digitalnih valuta su razvoj tehnologije i znanosti, kvalitativni i kvantitativni razvoj internetske mreže, razvoj kriptografije kao posebne znanstvene discipline te razvoj specifičnih tehnoloških rješenja kao što je na primjer Blockchain software.

[1] Sajter, D., „Financijska analiza kriptovaluta u odnosu na standardne financijske instrumente“, Financije- teorija i suvremena pitanja, EFOS, 2017
[2] Ibid.

Razvoj **telekomunikacijskih tehnologija** od kojih je internet sigurno najznačajnija infrastrukturna komponenta u masovnoj uporabi, odražava se na sve aspekte življenja, od tehnoloških do znanstvenih, ekonomskih, pa i socijalnih i psiholoških.

Bilo je samo pitanje dana kada će se početi koristiti i kao medij za ekonomske transakcije. Internet se osim po bou njegovih korisnika vremenom razvijao i u tehničkom smislu, brzina pristupa svakodnevno se povećava, kao i pristupačnost širenjem telekomunikacijskih mreža i razvojem tehnologije. U početnoj fazi, očekivano taj je trend, bio najsnažniji u najrazvijenijem dijelu svijeta. [3]

Kriptografija je multidisciplinarna znanost, bazirana uglavnom na područjima matematike i računalnih znanosti, u svrhu što efikasnijeg kodiranja i dekodiranja podataka. Razvojem računalne tehnologije, a posebno mikroprocesora, stvorili su se uvjeti za nastanak sve efikasnijih i bržih implementacija kriptografskih funkcija u računalnim funkcijama. Jedno od područja kriptografije je i razvoj tzv. hash funkcija. To su funkcije koje za ulaz mogu primiti niz podataka bilo koje duljine, i za njega će proizvesti specifičan „potpis" odnosno niz znakova unaprijed zadane duljine. Pri tome je važno da svaka i najmanja izmjena ulaznog niza znakova uzrokuje značajne promjene izlaznog niza, a brzina cijelog procesa direktno utječe na uporabljivost funkcije. Sama funkcija je „jednosmjerna" tj. lako je i brzo izračunati hash ulaznih podataka, ali je nemoguće iz hash-a dobiti originalni niz podataka. [4]

Ovakva tehnologija koristi se za osiguranje autentičnosti ili kontrolu podataka, na način da se provjerom potpisa (hash-a) koju je moguće lako i brzo izvršiti, može sa zadovoljavajućom razinom vjerojatnosti garantirati autentičnost originalnih podataka. Stoga je razvoj i unapređenje kriptografije svakako nužan preduvjet za razvoj novih elektroničkih sustava plaćanja i unapređenje njihove sigurnosti, a s tim i raznih oblika digitalnog novca.[5]

Blockchain je baza podataka u digitalnom obliku, koja sadrži dnevnik svih transakcija učinjenih u sustavu. Decentralizirana je u smislu da svaki sudionik sustava ima mogućnost pohraniti kod sebe vlastitu kopiju. Sudionici ili čvorovi u sustavu (eng. nodes) su ravnopravni svjedoci i kontrolori autentičnosti svake pojedinačne transakcije. Transakcije su grupirane kronološki, u tzv. blokove transakcija. Svaki blok transakcija digitalno je „potpisan" odnosno

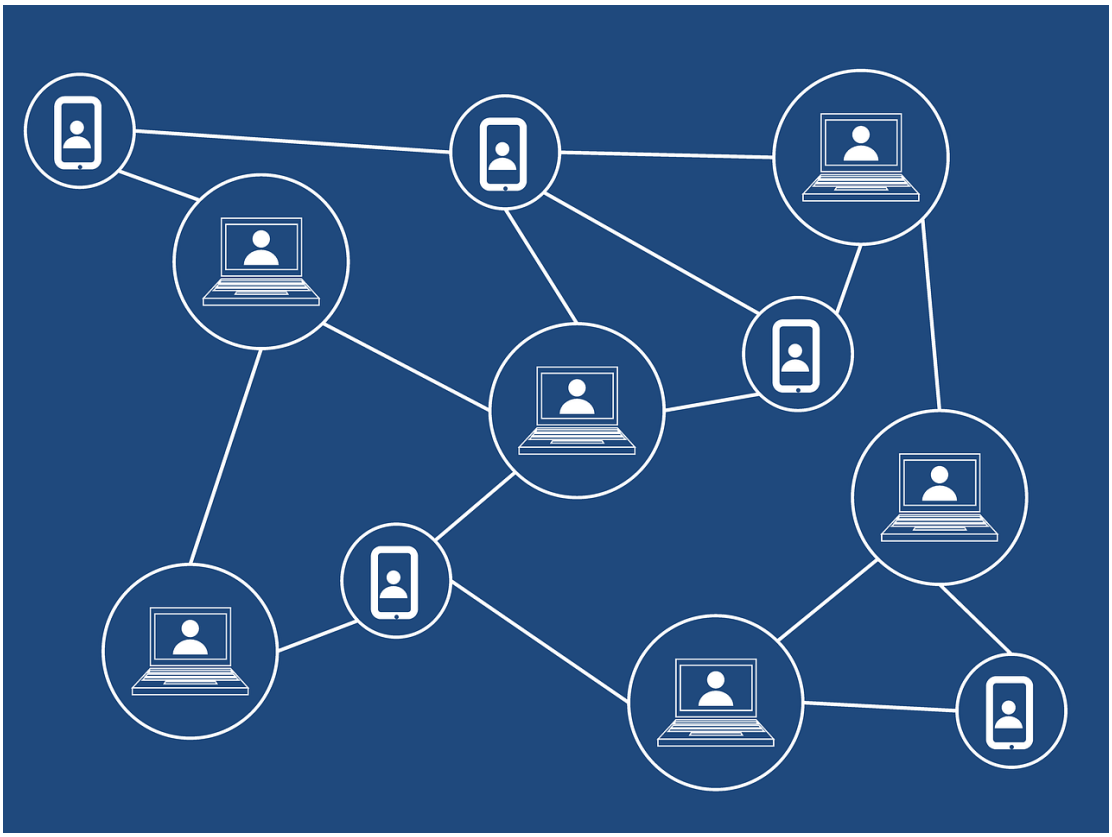
---

[3] CHENG, Cecilia, LI, Angel Yee-lam, Internet addiction prevalence and quality of (real) life: A meta-analysis of 31 nations across seven world regions, Cyberpsychology Behav. Soc. Netw., sv. 17, izd. 12, 2014, str. 755–760

[4] MIRONOV, Ilya, OTHERS, Hash functions: Theory, attacks, and applications, Microsoft Res. Silicon Val. Campus Noviembre De, 2005, Dostupno na: http://www.engr.uconn.edu/~akiayias/cse281sp08/CSE281_Computer_Security/Reading_files/hash_survey.pdf.

[5] BURR, William E., Selecting the advanced encryption standard, IEEE Secur. Priv., sv. 99, izd. 2, 2003, str.43–52

pridružena mu je određena digitalna šifra (eng. hash) koja je garancija da je blok autentičan, tj. svaki pokušaj promjene sadržaja bloka je vrlo lako otkriti. Uz navedeno, osim određenog broja transakcija, svaki blok sadrži i hash prethodnog bloka, što znači da ako netko želi promijeniti sadržaj određenog bloka (npr. dodajući ili mijenjajući transakcije), mora izmijeniti sve blokove u nizu nakon izmijenjenog bloka. Blokovi su na taj način povezani ili ulančani, odakle i potječe naziv Blockchain. Jedan od najboljih načina za shvatiti kako Blockchain funkcionira je obrada mentalne slike njegove strukture. Kao što njegov naziv implicira, Blockchain treba vizualizirati kao niz virtualnih kockica (zvanih Blocks) koji su poravnati u linearnoj, vertikalnoj strukturi. Prvi blok svih vremena, "majka svih blokova", nastao je 2009. godine i zove se Genesis Block. Nakon hijerarhijskog uređenja, svi blokovi stvoreni kasnije organizirani su u sukcesivnim razinama (ili slojevima u žargonu Blockchaina) koji odgovaraju njihovom vremenu stvaranja. Najnoviji blok uvijek je na vrhu lanca. Baš kao i generacije u obiteljskom stablu, Blokovi s istim roditeljskim blokovima smatraju se "braćom i sestrama" i leže na istom sloju. Slično ljudskoj DNK, svaki pojedini blok posjeduje jedinstveni identifikacijski kôd - zvan hash - od najviše 80 znakova. Štoviše, svaki blok sadrži i ID prethodnika u istom lancu.[6]



Slika 1. Izgled blockchaina

[6] Ibid

2.3. Različiti aspekti kriptovaluta

U radu kao primjer u proučavanju digitalnih valuta je najviše korišten Bitcoin, jer je trenutno najpopularniji predstavnik spomenutog koncepta, a zbog velike sličnosti (gledano u tehničkom, ekonomskom i pravnom smislu) većina izrečenog moglo bi se odnositi na bilo koju aktivnu digitalnu valutu baziranu na blockchain tehnologiji.

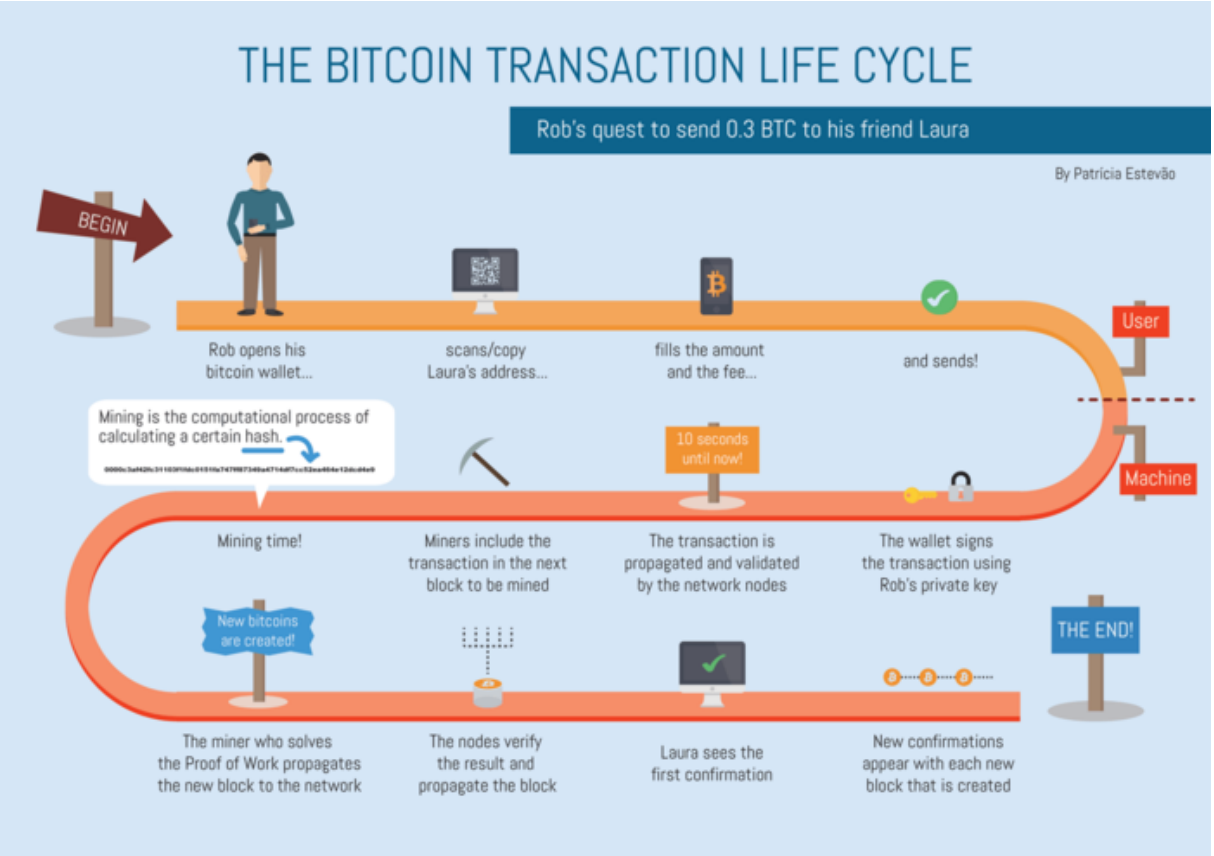
OBLICI VALUTA

Bitcoin zapravo nema materijalni oblik. Bitcoin adresa je oznaka ili broj koji možemo usporediti sa brojem klasičnog tekućeg računa u banci. Za svaku postojeću adresu sustav bilježi ulazne i izlazne transakcije, tako da zbroj svih transakcija predstavlja stanje na računu. Uz svaku adresu postoji i tzv. privatni ključ (eng. private key). Ako znate adresu, možete imati potpuni uvid u stanje, ali ne možete trošiti sredstva s računa. Za trošenje vam je potreban privatni ključ.[7] Možemo reći da je bitcoin zapravo broj računa (adresa) koji sadrži određeni saldo izražen u bitcoin jedinicama. Sastoji se od bitcoin adrese kao javnog dijela, i privatnog ključa koji omogućava trošenje. Bitcoin je zapravo informacija odnosno broj, koji predstavlja takozvanu bitcoin adresu, koja se može čuvati na više načina, najčešće u digitalnom obliku uz pomoć specijaliziranog računalnog programa. Takvi programi nazivaju se „novčanik“ (eng. Wallet) i pojavljuju se u više oblika odnosno inačica: za klasična stolna i prijenosna računala (software za Windows, Mac, Linux...), za mobilne uređaje (pametni telefoni i tableti, Android, iPhone...), kao web aplikacije (eng. Online web wallets), kao specijalizirani uređaji (eng. Hardware Wallets). Sve od navedenog ima određene prednosti i nedostatke a korištenje ovisi o osobnim preferencijama korisnika.[8]

Bitcoin **transakcija** realizira se u obliku razmjene poruka između pošiljatelja vrijednosti i sustava računala bitcoin mreže, tzv. skupina rudara (Mining pools) koji sudjeluju u procesu potvrde transakcija. Prilikom prijenosa određenog iznosa novčanih jedinica s jednog računa na drugi, računalni program elektroničkog novčanika prvo provjerava trenutno stanje salda korisnika, provjeravajući iznos na svakoj pojedinačnoj pohranjenoj adresi kako bi utvrdio postoji li dovoljna količina novca za realizaciju transakcije. Nakon toga, posebnim algoritmom pokušava se kombinirati traženi iznos iz postojećih adresa. Ukoliko je to kombiniranje moguće, transakcija se šalje svim čvorovima (eng. nodes) na potvrdu ili ovjeru. U slučaju da je nemoguće

[7] FAIRFIELD, Joshua AT, BitProperty, Cal Rev, sv. 88, 2014, str. 820
[8] Ibid.

iskombinirati traženi iznos, uzima se najbliži mogući veći iznos, a ostatak se kroz istu transakciju vraća pošiljatelju na neku od njegovih postojećih adresa.[9]



Slika 2. Bitcoin transakcija

Digitalne valute kao obračunske jedinice: Postoji vrlo malo podataka o bilo kojoj digitalnoj valuti koji bi upućivali na korištenje digitalne valute kao obračunske jedinice. Trgovci koji bi svoje cijene iskazivali u nekoj od digitalnih valuta, morali bi ih ažurirati vrlo često kako bi održali željenu vrijednost odnosno stabilnu cijenu u odnosu tradicionalne valute, npr. EUR ili USD. To je naravno posljedica visoke volatilnosti digitalnih valuta. Iako sve veći broj tvrtki radi olakšavanja plaćanja i pojednostavljenja iskazuju svoje cijene u npr. bitcoin-ima, to čine paralelno sa korištenjem klasičnih cjenika, koristeći digitalnu valutu kao privremeni medij plaćanja. Banke zapravo nisu svjesne ovih transakcija, jer u konačnici na račune dolazi klasični novac. [10]

Digitalne valute kao medij razmjene vrijednosti: Jedan od pokazatelja u kojoj mjeri se valuta koristi kao sredstvo razmjene je broj trgovaca koji su je spremni prihvatiti u plaćanju. Trenutno, postoji nekoliko tisuća trgovaca diljem svijeta (uglavnom, ali ne isključivo, internetskih

[9] ALI, Robleh i ostali, The economics of digital currencies, 2014, str. 279
[10] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/.

trgovina) koje primaju uplate u bitcoin-ima. Spremnost trgovaca da prihvate digitalnu valutu ne podrazumijeva da se ta mogućnost koristi. Bolji pokazatelj koliko određena digitalna valuta vrijedi kao sredstvo razmjene je broj transakcija provedenih od strane korisnika u određenom vremenskom razdoblju, kao i vrijednost ukupnog broja transakcija u određenom periodu. U tom smislu vidljiv je značajan trend porasta. Prema određenim dostupnim podatcima, vidimo da ukupna vrijednost dnevnog prometa prvih 100 najjačih digitalnih valuta premašuje 900 000 000 USD. [11]

Digitalne valute kao vrijednosti: Vrijednost novca općenito bazira se na sadašnjem i budućem vjerovanju korisnika u njegovu ponudu i potražnju. Kako u slučaju decentraliziranih digitalnih valuta ne postoji centralni autoritet koji ih kontrolira, njihova je vrijednost isključivo u povjerenju korisnika. Ponuda je uglavnom predvidljiva i relativno sigurna zahvaljujući ugrađenim mehanizmima, ali potražnja ovisi o više čimbenika i prilično je neizvjesna. Zbog toga digitalne valute zasigurno nisu pogodan medij za kratkoročno čuvanje vrijednosti. Što se tiče dugoročnog čuvanja vrijednosti, mišljenja su podijeljena. Prva koju čine formalne institucije i banke govori da su ulaganja u digitalne valute visoko rizična. Druga pak, kaže da se može očekivati velik porast vrijednosti, pa bi zato bilo zgodno ulagati u digitalne valute. Oba stava imaju određene argumente. U svakom slučaju, nedovoljna pravna reguliranost digitalnih valuta je već sama po sebi razlog za njihovo nekorištenje za dugoročnu čuvanje vrijednosti, osim u slučajevima spremnosti na visok špekulativni rizik. [12]

Danas prema mnogim izvorima na tržištu postoje preko 700 aktivnih, a računajući i one ugašene broj se penje značajno iznad 1000 valuta. Trenutno je još uvijek vidljiv trend porasta i broja valuta i tržišne kapitalizacije. Pri tome valja naglasiti da dobar dio valuta zbog vrlo male kapitalizacije nema ekonomskog značaja. Najbolji pokazatelji popularnosti digitalnih valuta su tržišna kapitalizacija i dnevni promet.

Ukupna kapitalizacija prvih 100 valuta iznosi više od 25 milijardi $. Za usporedbu, u veljači 2014. godine svega 34 valute vrijedilo je preko 1 mil. $. Aktualnim trendom, ukupna kapitalizacija se svake godine gotovo utrostruči. Mnoge valute nastaju gotovo svakodnevno, a samo one najlikvidnije predmet su trgovine na tržištu i nabrojane na coinmarketcap.com, dok su ostale izostavljene zbog premale likvidnosti. Međutim, postojanje mnogih nevažnih digitalnih valuta ne umanjuje činjenicu da važnost tzv. altcoin valuta raste u smislu alternativnih

[11] ALI, Robleh i ostali, The economics of digital currencies, 2014, str. 279
[12] Ibid.

investicijskih opcija. Altcoins se nazivaju alternativne implementacije digitalnih valuta baziranih na blockchain tehnologiji (alternativa bitcoin-u, odakle dolazi i naziv).[13]

PRISTUPANJE KRIPTOVALUTAMA

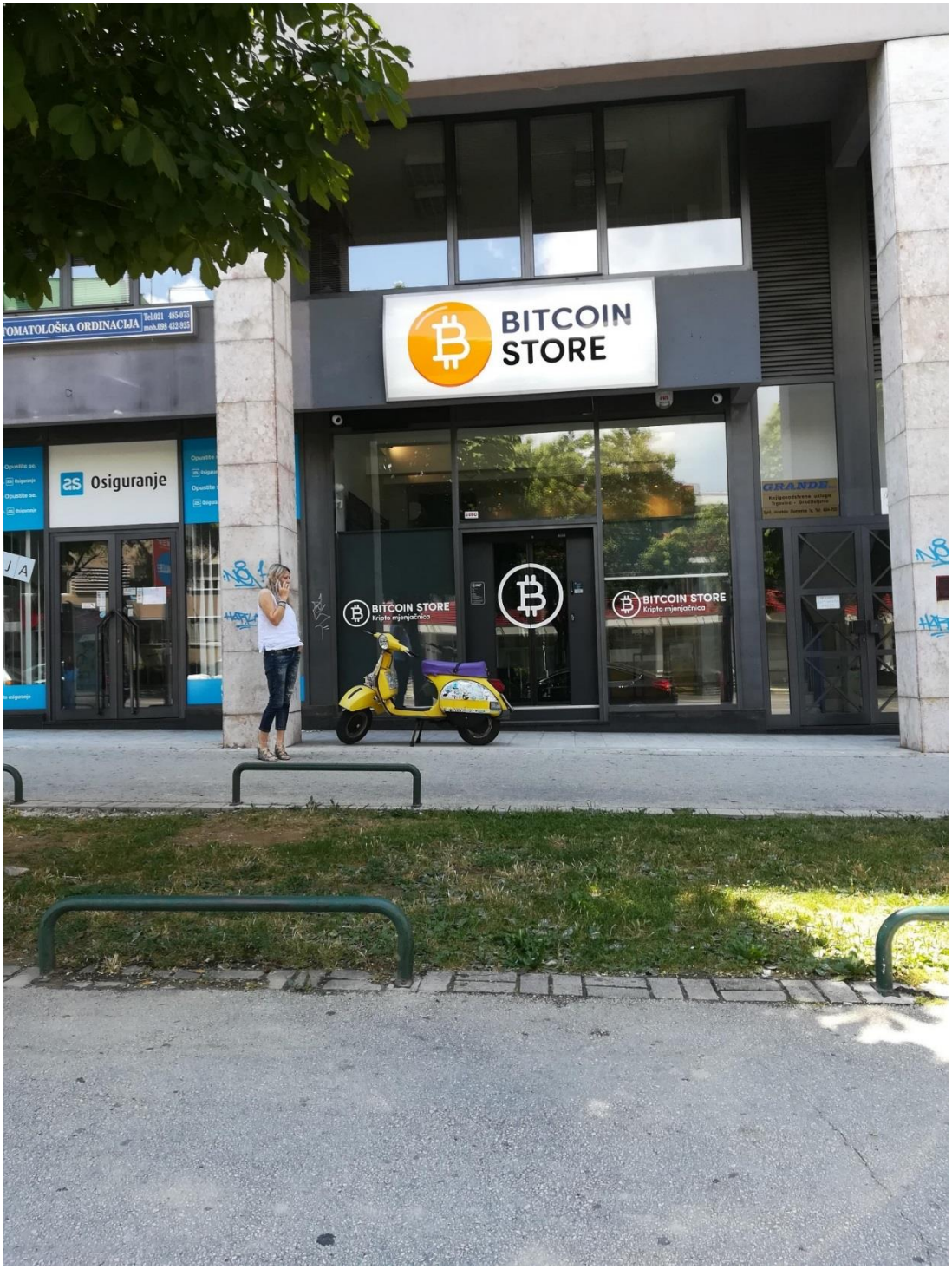
Uporaba digitalnih valuta, iako u snažnom porastu, još uvijek je ograničena na relativno mali udio populacije. Pretpostavka je da su to uglavnom korisnici koji dolaze iz tehničkih i financijskih područja djelatnosti, s određenom razinom tehničkih znanja, ali i razni drugi, entuzijasti željni upoznavanja novih tehnologija i špekulanti skloni podnijeti značajne rizike. Naravno, realno je pretpostaviti da postoji i određeni udio uporabe u ilegalne svrhe.

Kupnja Bitcoina nije uvijek jednostavna kao što možda očekuju novi korisnici. Dobra vijest je da broj opcija stalno raste. Neke čak ne moraju nužno zahtijevati elektronički novčanik ili pristup internetu. Osim dolje nabrojanih, ostale opcije uključuju Bitcoin debitne kartice, fizičke Bitcoin-ove „novčiće“ i tzv. prepaid kartice.[14] **Osobna prodaja** dostupna je za one koji žive u sredinama s većom koncentracijom korisnika, npr. u velikim svjetskim gradovima. Ovaj način prodaje omogućuje najnižu cijenu transakcije. Do određene mjere moguće je ostati anoniman. Postoje i određene internetske stranice koje olakšavaju pronalazak partnera za trgovinu.

Mjenjačnice za Bitcoin i ostale digitalne valute prisutne su u sve većem broju i realizirane gotovo u pravilu kao internetski servisi. Cijeli proces je moguće automatizirati, što se povoljno odražava na troškove. Najčešći načini plaćanja su kreditne kartice, Paypal i slični servisi elektroničkog plaćanja, te bankovni transferi. Provizije su relativno velike i najčešće se kreću u rasponu od 3-10% za kartice i Paypal, dok se kod bankovnih transfera može postići niži trošak. Prihvaćene su uglavnom najvažnije svjetske valute, USD, EUR, GBP i druge, dok korisnici ostalih manje značajnih valuta moraju prvo konvertirati svoje valute za neku koja se prihvaća u mjenjačnici. Što se anonimnosti tiče, ona u ovom slučaju nije moguća jer svaki od navedenih sustava plaćanja zahtijeva određeni oblik autorizacije. Pozitivno je što na ovaj način, a posebno kod plaćanja bankovnim transferima, postoji značajan stupanj sigurnosti. Mnoge mjenjačnice u ponudi imaju više aktivnih digitalnih valuta, te vrlo jednostavno i jeftino omogućuju njihovu zamjenu. Još uvijek nije lako kupiti Bitcoin-e kreditnom karticom ili PayPal-om. To je zato što se takve transakcije lako mogu poništiti telefonskim pozivom

[13] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/.
[14] COINDESK, How can I buy bitcoins?, CoinDesk, 20-kol-2013, Dostupno na: http://www.coindesk.com/information/how-can-i-buy-bitcoins/.

tvrtki za kartice (storniranje uplata). Budući da je teško dokazati da je bilo kakva roba promijenila ruke u prijenosu Bitcoina, mjenjači izbjegavaju takav način plaćanja i kao i većina privatnih prodavača. [15]



Slika 3. Bitcoin mjenjačnica

[15] Ibid.

Specijalizirani bankomati ukoliko su dostupni, jednostavna su i praktična opcija za trgovanje digitalnim valutama. Obavljanje transakcija je relativno brzo i jednostavno a postoji i mogućnost anonimnosti ako se plaća gotovinom. Provizije za Bitcoin se u najvećem broju slučajeva kreću u rasponu od čak 0,5% do 10%, ovisno o lokaciji i načinu plaćanja. Prosječna prodajna provizija je 6,01%, a kupovna 9,73%. Relativno niske provizije mogu se pronaći uglavnom samo na jako prometnim uređajima u zemljama sa velikom uporabom valute, kao što su Velika Britanija i SAD. Prema coinatmradar.com trenutno je evidentirano 1163 Bitcoin bankomata u svijetu.[16] Prema trenutnom trendu, svake godine broj se gotovo udvostruči. U Hrvatskoj je trenutno instalirano 3 uređaja, po jedan u Zagrebu, Rijeci i Splitu. Apsolutno najveći broj uređaja je u SAD-u.

Investicijski fondovi su još jedna zanimljiva mogućnost ulaganja u digitalne valute. Za korisnike koji žele uložiti u Bitcoin, a raspoložive metode im se čine komplicirane i nesigurne, ovakvi fondovi mogli bi ponuditi profesionalnu uslugu. Trenutno je poznato nekoliko pokušaja osnivanja takvih fondova, Bitcoin Investment Trust (BIT) i Winklevoss ETF , The Bitcoin Superfund . I u ovom slučaju nedostatak pravne definiranosti koči ovakvu inicijativu zbog osnovane bojazni vlasti o mogućnosti prevare.[17]

2.4. Primjeri kriptovaluta

BITCOIN

Bitcoin je **digitalni novac**, stvoren i čuvan elektronički. Bitcoin nije printan i **nije kontroliran** od strane bilo koga. Proizvode ga brojni ljudi pomoću računala u cijelom svijetu koristeći software koji rješava matematičke probleme. Bitcoin je prvi primjer ovakve valute nazvane **kriptovaluta** (*cryptocurrency*). Obzirom da je to tek početak revolucije digitalnog novca, bitcoin je najlakše objasniti uz pomoć klasičnog razvoja današnjih valuta kroz zlato. Bitcoin se koristi za kupovinu u elektroničkom obliku. U tom se smislu ne razlikuje ni od jedne druge valute (kune, dolara, eura…) kojom se također trguje digitalno.

[16] Bitcoin ATM Map, Dostupno na: https://coinatmradar.com/.

[17] BUKHARI, Jeff, Bitcoin: Winklevoss ETF May Not be Dead Yet, Fortune, Dostupno na: http://fortune.com/2017/03/23/why-the-winklevoss-bitcoin-etf-may-not-be-dead-yet/

Međutim, bitcoinova najznačajnija karakteristika i ujedno najveća razlika od ostalih valuta jest što je decentraliziran. Niti jedna institucija ne kontrolira bitcoin mrežu. Trenutni pobornici bitcoina to smatraju enormnim plusom, budući da do oscilacija vrijednosti dolazi jedino zbog ljudi. Bitcoin je nastao kao produkt ideje software developera Satoshi Nakamoto-a; elektroničko plaćanje na temelju matematičkih dokaza. Ideja mu je bila stvaranje valute bez centralne vlasti, s elektroničkim prijenosom (i to uglavnom instantnim), s vrlo malim ili nikakvim transakcijskim troškovima. Zbog toga bitcoin ne izdaje nitko. Bitcoin nije fizički izdan u sjeni centralnih banaka, gdje ga ljudi ne mogu prebrojati i gdje banke postavljaju svoja pravila. Upravo te banke, kada upadnu u dug, jednostavno izdaju više novca što rezultira smanjenjem vrijednosti novca, tj. inflacijom. Umjesto toga, bitcoin je stvoren digitalno, od strane zajednice kojoj se svatko može pridružiti. Bitcoinovi su rudareni (Mined) pomoću računala, tj. korištenjem procesorskog vremena i distribuirani u bitcoin mreži. Mreža također procesira transakcije napravljene pomoću bitcoina, što rezultira stvaranjem vlastite platne mreže. Bitcoin protokol, tj. algoritam pomoću kojeg cijeli sustav funkcionira, ograničen je na izdaju 21 milijuna bitcoinova. Međutim, svaki bitcoin ima puno veću vrijednost nego tradicionalna valuta te je zbog toga podijeljen na manje dijelove, od kojih je najmanja milijunti dio, "Satoshi", nazvan po izumitelju bitcoina. Tradicionalne valute nekoć su se temeljile na zlatu i srebru. Teoretski, znali ste da ćete za 100 dolara dobiti određenu količinu zlata (iako to nije funkcioniralo u praksi). Bitcoin nije temeljen na zlatu, već ovisi o matematici. Diljem svijeta ljudi koriste program koji slijedi matematičku formulu za proizvodnju bitcoina. Ta formula je javno dostupna svima, jer je napisana OpenSource kodom, tako da svatko može pogledati i uvjeriti se da radi ono za što je i stvoren.[18]

Slika 4. Bitcoin u fizičkom i digitalnom obliku

[18] https://crobitcoin.com/bitcoin/sto-je-bitcoin/

ETHERUEM

Blockchain tehnologija postala je poznata preko Bitcoina, no ima **razne druge mogućnosti koje proizlaze okvire digitalne valute**. Bitcoin nije jedina implementacija koja koristi blockchain tehnologiju, svakim danom se javljaju nove kreativne aplikacije koje iskorištavaju prednosti blockchaina.

Prije Ethereuma, izrada aplikacija nad blockchainom je zahtijevala veliko iskustvo u programiranju, kriptografiji, matematici… U to vrijeme su mnoge ideje za iskorištavanjem blockchain tehnologije djelovale kompleksno pa nerijetko čak i nemoguće. S razvojem Ethereuma, **sve te nemoguće aplikacije su ugledale svjetlo dana**. Ethereum je omogućio da razne ideje mogu biti razvijene izrazito brzo i kvalitetno korištenjem njihovog blockchaina. Ethereum je otvorena platforma bazirana na blockchain tehnologiji koja omogućuje programerima da razvijaju i objave decentralizirane aplikacije.

Isto kao i Bitcoin, Ethereum je javna distribuirana blockchain mreža. Iako postoje neke bitne razlike u njihovoj tehničkoj izvedbi, **najveća je razlika u njihovoj svrsi te mogućnostima**. Bitcoin je jedna specifična aplikacija koja koristi blockchain tehnologiju, distribuirani sustav elektroničkog novca koji omogućuje plaćanje i transfere pomoću Bitcoina. Dok je Bitcoin blockchain mreža korištena za kontrolu tko posjeduje koliko elektroničkog novca Bitcoin, Ethereum blockchain mreža je fokusirana na pokretanje programskog koda bilo koje decentralizirane aplikacije.

U Ethereumovom blockchainu, umjesto rudarenja Bitcoina, rudari rade kako bi zaradili Ether, **tip digitalne valute koji služio kao gorivo za njegovu blockchain mrežu**. Osim da bi bio prodan na nekoj burzi, Ether se koristi u Ethereum blockchainu kako bi se platile naknade i usluge koje se koriste.

Ruski programer Vitalik Buterin kreirao je Ethereum krajem 2013-te. Vitalik je najavio Ethereum u Siječnju 2014 na The North American Bitcoin konferenciji u Miamiju, US. Njegov kreator **Vitalik je toliko vjerovao da blockchain tehnologija može promijeniti svijet da je odustao od fakulteta** da bi se u potpunosti mogao posvetiti razvoju Ethereumu. Ethereum je kreiran da napravi stvari koje su bile nemoguće s Bitcoinom. Cijela ideja oko Ethereuma nije da bude samo još jedna kripto valuta već da bude više od toga, puno više.

Pametni ugovor je zapravo pojam koji se koristi za računalni program koji služi za olakšavanje razmjene kao što su novac, sadržaj, nekretnina, udjeli ili nešto drugo što predstavlja nekakvu razmjenu vrijednosti. Kada se pametni ugovor izvršava na blockchain mreži on **postaje računalni program koji se samostalno izvršava** kada su određeni preduvjeti zadovoljeni.

Bitno je napomenuti da u slučaju da se računalni program izvršava na blockchainu nije moguće raditi nikakve promjene kao što su cenzuriranje, malverzacije ili uplitanje neke treće strane, izvršava se točno onako kako je programiran.
Sve blockchain mreže imaju sposobnost izvršavanja računalnog koda, ali većina je limitirana na neki način. Naime, Ethereum blockchain je drugačiji. Umjesto da su dozvolili limitirani skup operacija, **Ethereum je kreiran s idejom da se programerima koji će raditi nad platformom dopusti korištenje bilo koje operacije**. To znači da programeri mogu razvijati tisuće različitih aplikacija koje prelaze limite koji su do sada postojali u primjeni blockchain tehnologije. Prije kreiranja Ethereuma, blockchain aplikacije su bile dizajnirane sa svega nekoliko operacija. Bitcoin je razvijan ekskluzivno za primjenu operacija koje su nužne isključivo za transfer elektroničkog novca.
Programeri su se suočili s problemom. Postojale su dvije opcije, jedna od njih je da prošire izvorni kod od Bitcoina proširen s operacijama koje njima trebaju, ali to je bila dugotrajna i komplicirana opcija. **Druga opcija je bila da razviju novi blockchain kao zasebnu platformu**. Skupina programera se odlučila za ovaj drugi pristup te je stvoren Ethereum. Glavna inovativnost Ethereuma je njegovo virtualno računalo (EVM) koja je ključna za izvršavanja kompletnog računalnog programa u Ethereum mreži. To je omogućilo bilo kome da kreira bilo koju aplikaciju i pusti je u mrežu. Ethereum virtualno računalo je po prvi puta omogućila proces kreiranja blockchain aplikacija na vrlo jednostavan i učinkoviti način. Prije je bilo potrebno napraviti cijelu blockchain mrežu za svaku pojedinu aplikaciju, Ethereum je omogućio da se taj korak izbjegne i bilo koja aplikacija može koristiti njegovu mrežu. Ethereum omogućuje programerima da razvijaju i lansiraju decentralizirane aplikacije. Decentralizirana aplikacija predstavlja samo jednu aplikaciju koja služi za neku posebnu namjenu, te ima određenu svrhu za svoje korisnike.
Na primjer, Bitcoin je decentralizirana aplikacija koje omogućuje korisnicima da koriste neku verziju elektroničkog novca te rade novčane transakcije preko nje. Decentralizirane aplikacije su napravljene od izvornog koda koji se pokreće i izvršava na blockchain mreži, nije moguće kontrolirati njegovo ponašanje preko nekog centraliziranog entiteta.
Bilo koja centralizirana aplikacija ili usluga može biti decentralizirana pomoću Ethereuma. Podizanje kredita od strane banke, registracija korisnika u nekakvom registru, online glasanje itd.
Vrijednost Ethereuma je doživjela drastičan rast u proteklih godinu dana, svi pričaju o Bitcoinu, ali Ethereum mu je za petama. Prošle godine ste **mogli kupiti Ethereum za $10, ali sada, za**

to trebate uložiti više od $300. Iako je Bitcoin za mnoge sada postao već preskup, Ethereum ima potencijala da probije $1000, a trenutno je i dalje relativno pristupačan.[19]

Slika 5. Fizički oblik Ethereuma

[19] https://crobitcoin.com/altcoin/ethereum/

3. OPERATIVNE TRANSAKCIJE KRIPTOVALUTAMA

Kao primjer u proučavanju je najviše korišten Bitcoin, jer je trenutno najpopularniji predstavnik spomenutog koncepta, a zbog velike sličnosti većina izrečenog moglo bi se odnositi na bilo koju digitalnu valutu baziranu na blockchain tehnologiji.
Osnovne razlike među pojedinim valutama su uglavnom u specifičnostima tehničke prirode, te u prihvaćenosti pojedine valute, odnosno tržišnoj kapitalizaciji.

3.1. Oblici digitalnih valuta

Bitcoin nema materijalni oblik, iako se može prikazati i čuvati na materijalnom mediju (npr. papiru). Pri tome fizički oblik nema nikakvu važnost niti vrijednost, kao što je to slučaj kod klasičnog novca, gdje sama novčanica u fizičkom smislu predstavlja vrijednost i kao takva se ne može (legalno) kopirati. Bitcoin adresa je oznaka ili broj koji možemo usporediti sa brojem klasičnog tekućeg računa u banci. Za svaku postojeću adresu sustav bilježi ulazne i izlazne transakcije, tako da zbroj svih transakcija predstavlja stanje na računu. Pri tome se ne čuvaju salda pojedinih računa nego povijest svih transakcija, iz kojih se može lako izračunati trenutni saldo za svaku adresu. Uz svaku adresu postoji i tzv. privatni ključ (eng. private key). Ako znate adresu, možete imati potpuni uvid u stanje, ali ne možete trošiti sredstva s računa. Za trošenje vam je potreban privatni ključ. [20]
Dakle, možemo reći da je bitcoin zapravo broj računa (adresa) koji sadrži određeni saldo izražen u bitcoin jedinicama. Sastoji se od bitcoin adrese kao javnog dijela, i privatnog ključa koji omogućava trošenje.
Na slijedećoj slici vidimo primjer Bitcoin-a tiskanog na papiru.

Slika 6. Bitcoin na tisakanom papiru

[20] FAIRFIELD, Joshua AT, BitProperty, Cal Rev, sv. 88, 2014, str. 820

Glavni dio je privatni ključ i bitcoin adresa (javni ključ) koji se jednostavno mogu prepisati na običan papir a da ne izgube vrijednost. Privatni ključ potrebno je čuvati u tajnosti, jer omogućava otuđenje vrijednosti sa računa (adrese). Javni ključ ili adresa mogu se dijeliti u javnosti i potrebni su onome tko želi doznačiti sredstva na račun (adresu).
Svaka bitcoin adresa i pripadajući privatni ključ su međusobno povezani na način da je adresa rezultat određene kriptografske funkcije provedene nad privatnim ključem. Znači da znajući adresu ne možemo utvrditi privatni ključ, ali znajući privatni ključ, možemo utvrditi adresu odnosno račun vlasnika.[21]
Prilikom provjere svake transakcije, sustav uz pomoć privatnog ključa provjerava pripada li odgovarajuća adresa ključu, a zatim raspolaže li adresa sa dovoljno novca za izvršenje transakcije (je li saldo zadovoljavajući).

3.2. "Novčanici"

Bitcoin je zapravo informacija odnosno broj, koji predstavlja bitcoin adresu, koja se može čuvati na više načina, najčešće u digitalnom obliku uz pomoć specijaliziranog računalnog programa. Takvi programi nazivaju se „novčanik" (eng. Wallet) i pojavljuju se u više oblika odnosno inačica:

1. Za stolna i prijenosna računala (software za Windows, Mac, Linux...)
2. Za mobilne uređaje (pametni telefoni i tableti)
3. Kao web aplikacije (eng. Online web wallets)
4. Kao specijalizirani uređaji (eng. Hardware Wallets)

Moderni bitcoin novčanici raspolažu sa više korisnih funkcija. U njima možete čuvati podatke o puno adresa i pripadajućih ključeva, automatski će vam prikazivati ukupno stanje salda, vršiti provjeru transakcije prije nego je pošalju u sustav itd.
Najviše funkcija imaju novčanici za **klasična računala**. Mnogi od njih su u mogućnosti čuvati cjelokupnu bazu podataka svih transakcija i u stvarnom vremenu vršiti provjere pojedinih transakcija preko priključenih čvorova mreže. Na taj način moguće je pružiti zadovoljenje najviših sigurnosnih standarda u tehničkom smislu, jer nisu potrebni kompromisi oko veličine uređaja, količine memorije, potrošnje energije, brzine interneta i slično. Osnovni nedostatak je što nisu uvijek dostupna, kao i praktična za prenošenje.
Ovdje dolazimo do **mobilnih uređaja ili pametnih telefona**. Uz korištenje mnogobrojnih

[21] DOWD, Kevin, HUTCHINSON, Martin, Bitcoin will bite the dust, Cato J, sv. 35, 2015, str. 359,364

mobilnih aplikacija ovi uređaji poprimaju sve više funkcija, pa tako i bitcoin novčanika. Ovako implementirana rješenja vrlo su praktična i dostupna. Funkcionalnost u nekim slučajevima i nadmašuje onu kod klasičnih računala, jer su dostupne kamere za skeniranje kodova, te moderna NFC tehnologija za bez-kontaktno plaćanje. Nedostatak je što se mobilni uređaji lako izgube ili bivaju ukradeni, pa se na taj način gubi i vrijednost u njima.

Web aplikacije u funkciji novčanika vrlo su praktične. Sadrže sve prednosti klasičnih novčanika uz nemogućnost gubljenja i izuzetnu dostupnost, svuda gdje postoji pristup internetu. Sredstva su uvijek i svuda dostupna, nije potrebno imati posebne uređaje, niti ih moramo posjedovati, web novčanici pristupačni su sa svakog računala spojenog na Internet. Nedostatak ovih rješenja je pouzdanost, odnosno potrebno je imati povjerenje u organizaciju koja nudi navedene usluge. U slučaju da sustav nije dobro osiguran, postoji opasnost od krađe. Specijalizirani uređaji u funkciji novčanika po svojim prednostima i nedostacima mogu se usporediti sa onima za pametne telefone, pa za njih vrijedi isto što i za mobilne uređaje. Zapis adresa na bilo kakvom mediju je još jedna od opcija. Bitcoine možete jednostavno isprintati na papir i kako takve čuvati na načine kako se čuvaju klasične papirne novčanice.[22]

3.3. Transakcije

Bitcoin transakcija realizira se u obliku razmjene poruka između računala platitelja odnosno pošiljatelja vrijednosti i sustava računala bitcoin mreže, tzv. skupina rudara (Mining pools) koji sudjeluju u procesu potvrde transakcija. Komunikacija se odvija putem standardnog internetskog komunikacijskog protokola u šifriranom obliku. Komunikacijski protokol je detaljno definiran i javno dostupan svima. Ovdje će biti prikazani samo najosnovniji principi, kako bi se moglo pristupiti analizi primjenjivosti i omogućiti korištenje na zadovoljavajućem sigurnosnom nivou.

Prilikom prijenosa određenog iznosa novčanih jedinica s jednog računa na drugi, računalni program prvo provjerava trenutno stanje salda korisnika, provjeravajući iznos na svakoj pojedinačnoj pohranjenoj adresi kako bi utvrdio postoji li dovoljna količina novca za realizaciju transakcije. Kada se utvrdi saldo, posebnim algoritmom pokušava se kombinirati traženi iznos iz postojećih adresa. Ukoliko je to kombiniranje moguće, transakcija se šalje svim čvorovima (eng. nodes) na potvrdu ili ovjeru. U slučaju da je nemoguće iskombinirati traženi iznos, uzima se najbliži mogući veći iznos, a ostatak se kroz istu transakciju vraća pošiljatelju na neku od njegovih postojećih adresa.

[22] www.kriptovalute.hr

Na prethodnoj se slici vide tri transakcije. Lijevo od zelene strelice su adrese sa kojih se šalje određeni iznos novca na adresu ili adrese s desne strane. Vidljivo je kako se pojedina transakcija često odvija između nekolicine polaznih i najčešće dvije dolazne adrese, jedna primatelja novca i druga pošiljateljeva radi povrata viška iznosa. Treća transakcija je primjer s povratom dijela iznosa na istu adresu s koje je izvršen transfer.[23]

3.4. Potvrda transakcija

Svaki mrežni čvor sustava odnosno „rudar“ (eng. miner) stalno je spojen na internetsku mrežu i prima sve novo emitirane transakcije svih korisnika (odnosno njihovih novčanika). Primljene transakcije spremaju se u memorijski prostor primatelja (eng. memory pool) gdje čekaju da budu zapakirane u novi blok transakcija, ovjerene i dodane u centralni dnevnik transakcija. Dodavanjem bloka u centralni dnevnik (blockchain) sve transakcije u bloku su ovjerene, transparentne i može ih provjeriti bilo tko. Svakim dodavanjem novog bloka u centralni dnevnik višestruko se ovjeravaju sve transakcije prethodnih blokova, povećavajući sigurnost sustava i u tehničkom smislu onemogućavajući zlouporabu cijelog sustava. Svaki rudar prilikom formiranja novog bloka transakcija, osim samih transakcija, oznake bloka, potpisa prethodnog ovjerenog bloka itd. u blok ugrađuje i jedan proizvoljan broj (u eng. jeziku nazvan nonce), promjenom kojega (pošto su sve ostale komponente bloka strogo definirane) može utjecati na potpis (eng. hash) samog bloka. Sustav je projektiran tako da zahtjeva hash manji od zadane vrijednosti. Kako nije moguće predvidjeti izlaznu vrijednost hash funkcije, rudari je moraju pogađati, odnosno ponavljati izračun mijenjajući nonce vrijednost, sve dok ne dobiju zadovoljavajući hash. Prvome koji dobije zadovoljavajući hash, sustav dozvoljava upis novog bloka u centralni blockchain, i nagrađuje ga određenom količinom novostvorenih novčanih jedinica. Na taj način motiviraju se rudari za svoj doprinos i istovremeno u opticaj pušta nova količina novca.

Brzina kojom se dodaju novi blokovi u centralni dnevnik sustavno je regulirana i podešena na približno 10 minuta. Ona ovisi o ukupnoj procesorskoj snazi sustava koji računa hash (eng. hashrate) i težini zadatka, odnosno zahtijevajući hash manji od određene vrijednosti. Ukoliko se hashrate sustava ubrza i novi blokovi počnu pristizati brže, sustav se automatski korigira povećavajući težinu zadatka sve dok ne postigne željenu brzinu zapisa od jednog bloka svakih 10 minuta. To znači da za potvrdu bitcoin transakcije treba čekati bar 10 minuta, a ako se radi o većim transakcijama, preporuka je čekati nekoliko (5-6) potvrda, što znači

[23] Ibid

približno 1 sat. Ovako dugo vrijeme ovjere transakcije jedan je od najjačih odbijajućih tehničkih čimbenika za prihvaćanje blockchain tehnologije od strane banaka.

Ovakav način potvrde transakcija naziva se eng. Proof of work ili skraćeno POW, zato što je potrebno uložiti određeni računalni rad kako bi se blok transakcija potvrdio. Uloženi rad ujedno je i garancija autentičnosti zapisa, odnosno sigurnosni čimbenik. U teoriji, za zapis lažne transakcije u sustav potrebno je raspolagati sa više od pola ukupne procesorske snage sustava. To je u praksi teško postići i o tome pišu brojne studije. Prema nekim autorima, ako bi netko kontrolirao više od pola čvorova na mreži, vrlo vjerojatno ne bi imao motiv raditi kriminalne radnje jer bi na taj način utjecao na pad vrijednosti valute zbog čega bi i sam najviše izgubio. Sustav bi tada pokazao tendenciju prijelaza u centralizirani, pa bi primjena blockchain tehnologije izgubila smisao.

Brojni stručnjaci nastoje razviti i unaprijediti sustav koji koristi POW, zbog njegovih glavnih nedostataka; vremena za potvrdu transakcija i potrebe za „rudarima“ te potrošnjom električne energije. Iz tog razloga javljaju se alternativna rješenja korištena u mnogim novim digitalnim valutama.[24]

[24] Ibid.

4. PRIMJERI KORIŠTENJA KRIPTOVALUTA U POSLOVANJU

4.1. Primjeri iz međunarodnog poslovanja

Bitcoin i etherium se najviše koriste u međunarodnom poslovanju u zabilježenim slučajevima. Prednost korištenja kriptovaluta u međunarodnom poslovanju očituje se kroz izbacivanje posrednika, a samim time transakcija postaje puno jeftinija, što je najveća prednost korištenja kriptovaluta.

Najpopularniji oblici plaćanja na internetu su kreditne kartice koje su se unaprijedile u zadnjih godina, ali su podložne i prevarama, te Paypal.

Na primjer, dvije kompanije otvore svoje kriptovalutne lisnice koje će koristiti kao pravne osobe, Fizičke ili pravne osobe nisu baš relevantne kad su u pitanju kriptovalute. Kompanije se međusobno dogovore oji će on line servis isplate kriptovaluta koristiti i ta se kriptovauta prebacuje na bankovni račun. Nakon toga se dobije potvrda o završetku transakcije.

U međunarodnom poslovanju dobar temelj za korištenje kriptovaluta bi se sagradio u slučaju stvaranja kriptovalute pod državnim pokroviteljstvom. Prema Deloitteovoj studiji djelovalo bi slično kao i bitcoin: „pojedinci ili kompanije bi koristili računalno-generirane javne ‘adrese’ za slanje i dobivanje isplata. Platitelji bi mogli koristiti elektroničku lisnicu na pametnom telefonu ili računalu za slanje novca prema javnim adresama primatelja. Za razliku od trenutnog sistema kojeg koristi bitcoin, banke i druge financijske institucije, prethodno odobrene od strane središnje banke, bi bili zaduženi za zbrinjavanje blockchain varijacije. Valuta u registratoru bi bila jedna od postojećih fiat valuta, umjesto neke nove nesigurne digitalne valute”.

Izvještaj pod imenom Disruptive Technology: Bitcoins, Currency Reinvented koji je izdao Kuvajtski financijski centar istražuje mogućnost upotrebe bitcoina za izvoz, pogotovo nafte. Treba istaknuti da je oko 80 % zaljevske ekonomije ovisno o nafti i njenim derivatima. Izvještaj se fokusirao na mogućnost upotrebe bitcoina za prodaju izvoz nafte, upravo zbog tog razloga. Ta studija stvara važan temelj za istraživanje alternativnih opcija plaćanja u slučaju da američki dolar prestane biti preferirana valuta za trgovinu nafte.

Jedan startup iz Hong Konga je došao na ideju da napravi kompletno novu kriptovalutu kojom će osiguravati prijevoz i kontrolu brodskih kontejnera. Smatraju da će rezervacija depozita u vidu kriptovalute biti potrebno rješenje za jednu od najvećih boljki unutar transportne industrije, a to je povjerenje, odnosno njegov nedostatak. Commonwealth Bank of Australia i Wells Fargo & Co su bili akteri prve prekogranične transakcije između banaka koristeći blockchain tehnologiju, koja je rezultirala transportom pamuka iz Kine do SAD-a. Riječ je o skupu

komplementarnih tehnologija i tehnoloških pravaca koji imaju moć promijeniti svijet međunarodne trgovine.

Potrebno je izdvojiti i jedan B2G slučaj. Propy, blockchain startup vezan za nekretnine dogovorio je suradnju s ukrajinskom vladom za projekt decentraliziranog tržišta nekretnina. Omogućuje stranim investitorima da kupuju nekretnine koristeći platformu baziranu na Etheriumu

Sandeep Goenka, suosnivač Zebpaya, mobilne aplikacija za prodaju i kupovinu bitcoina, govori da: „Bitcoin je bez granica, isto kao i internet. Ako želite obaviti inozemnu uplatu, slanje bitcoina je jednostavno poput slanja e-maila. Mislim da je korištenje bitcoina za B2B i dalje par godina udaljeno zbog regulatorne konfuzije. Freelanceri u Indiji već koriste bitcoin umjesto Paypala i Western Uniona za zaprimanje manjih isplata od njihovih inozemnih klijanja za web dizajn i slično. Uštede tih 10–15 % koje inače ove kompanije naplaćuju. Također, dobiju novac instantno umjesto da čekaju 7–15 dana".[25]

SIGURNOST TRANSAKCIJA

Blockchain je pozadina koja osigurava nesmetanost i sigurnost prijenosa i izvršenja nekog posla. Smatra se da bi blockchain mogao kompletno revolucionalizirati financijski svijet i usluge, pogotovo zbog svoje decentralizirane prirode. Blockchain nudi mogućnosti koje su koje imaju veliku primjenu u međunarodnom poslovanju.

Prva banka u Švicarskoj koja je omogućila svojim klijentima da kupuju, prodaju i drže bitcoin je Falcon Private Bank. Bitno je naglasiti da banka ima podršku Švicarske FINMA-e, državnog tijela za financijskog regulacije s regulatorne strane, a s kriptografske strane od kompanije Bitcoin Suisse AG.

Jedan ruski konzorcij banaka odlučio je koristiti blockchain zasnovan na prethodno spomenutom Ethereumu kako bi uplate bile sigurnije i brže. Banke, uključujući VTB Group i Sberbank PJSC stvorile su distribuirani registar pod imenom Masterchain koji koristi modificirani Ethereum protokol. Registar spada pod državne sigurnosne standarde, prema procjeni FinTech Associationa, kojeg podupire središnja banka.

Korištenje kriptovaluta nikad nije potpuno sigurno, uvijek postoji rizik.

Najistaknutiji primjer za spomenutu nesigurnost jest pad i fijasko vezan za najveću burzu bitcoina zvanu Mt.Gox. Američki federalni agenti, s poprilično utemeljenim dokazima u vidu zamračene imovine i transakcija, optužili su Alexandera Vinnika da je ukrao i pronevjerio preko

[25] Turudić, Milić, Štulina, Korištenje kriptovaluta u međunarodnom poslovanju; Zbornik radova Libertas sveučiliša; Zagreb, 2017

800 000 bitcoina, čija je vrijednost u američkim dolarima tada bila oko 400 milijuna. Menadžment Mt. Goxa je veoma loš, pogotovo u vidu sigurnosti. Odgovorni Mark Karpeles je vodio užasan posao u upravljanju burzom i financijama, zbog čega je jedan od najvećih projekata u povijesti kriptovaluta neslavno propao.[26]

4.2. Primjeri iz poslovanja Hrvatske

Republika Hrvatska sporo prihvaća nove tehnologije. Po potanju kriptovaluta, Rh je otvorio nekolicine bankomata u Zgarebu, Rijeci i Splitu. Prema Heidu, „regionalna nestabilnost i građanski nemiri diljem svijeta su tradicionalno manifestirali interes za tržište metala, uzrokovajući značajan rast u cijenama metala jer je populacija svoju imovinu pretočila u zlato i srebro u slučaju da fiat valute propadnu. S druge strane im je to napravilo problem jer je novonastala imovina bila teško prenosiva, u slučaju da su lokalne političke okolnosti postale previše opasne za život i zahtijevale su mijenjanje geografske lokacije".

Stranica poslovni.hr nudi primjer prodaje kriptovalute u Republici Hrvatskoj kada je Xaurum Gamma, prvi građevinski i turistički projekt u Hrvatskoj iskoristio grupno financiranje pomoću kriptovaluta (Initial Coin Offering - ICO) kao način prikupljanja kapitala, koji nije uspio i ugasio se. Villa Rustica ili Gama Rustica, kako se naziva na Booking.comu, raskošna vila s bazenom i jacuzzijem smještena u mjestu Linardići na otoku Krku, stavljena je na prodaju.
Voditelj projekta, Auresco institut iz Ljubljane, koji u Hrvatskoj posluje preko tvrtke Gama gradnje, objavio je na svojim internetskim stranicama da investitorima vraća puni iznos uloženih sredstava. "Nakon pažljivog razmatranja, odlučili smo da se zaustavi sve aktivnosti vezane uz projekt Xaurum Gamma (X-Gamma) što trenutačno vidimo kao jedinu logičnu i realističnu opciju da bi se spriječila eventualna šteta ulagačima i da njihov novac ostane netaknut", poručuju voditelji projekta.
Investitori su bili slovenski državljani. Auresco institut objavljivao je na svojim internetskim stranicama da je kroz ICO skupljeno 2,06 milijuna eura kapitala, a u međuvremenu taj se iznos spustio na milijun eura. Za uspjeh projekta trebalo je barem pet milijuna eura kapitala. Xaurum Gamma zamišljen je kao kompleks šest luksuznih vila koje bi se temeljile na blockchainu. Prema riječima Jakob Kapusa iz Auresca svaka je vila trebala biti upisana na blockchain.

[26] Ibid

Trebale su imati zasebnu blockchain adresu preko koje bi investitori mogli pratiti sve transakcije iznajmljivanja vila. Na blockchain su trebali biti zapisani i automobili, plovila, katering usluge, dostave dronom i ostala imovina i usluge, uključujući usluge čišćenja i održavanja, a koje su planirali iznajmljivati i prodavati turistima. "Primjer je to ekonomije u realnom vremenu, gdje investitori mogu u svakom trenutku vidjeti što se događa s projektom", istaknuo je tada Kapus.

Villa Gamma Rustica, prva od njih šest, bila je dovršena prošlu godinu i odmah je stavljena u pogon. Iznjamljivala se i preko Booking.coma. Ali, sada na tom servisu stoji obavijest da nove rezervacije za taj objekt ne primaju. Projekt je pravno bio reguliran na neuobičajen način. Načelno ga je vodio slovenski Auresco institut. U Hrvatskoj je tu operaciju vodio preko tvrtke "Gama gradnje", a plan je bio, da kad vile budu gotove, da ih se stavi na upravljanje Gamma Trustu sa sjedištem u Lihtenštajnu. Lani se na internetskim stranicama projekta moglo vidjeti da su dvije vile u procesu gradnje. Voditelj projekta zaključuje da je projekt zaustavljen u travnju, jer na njemu gube novac.[27]

Hrvatska je među državama koje imaju svoj bitcoin bankomat, kojih je tek nešto više od 300 u svijetu. Postavljen je u Zagrebu u Tkalčićevoj ulici, a prema dostupnim podacima, posluje dobro.

Smatra se kako je u Hrvatskoj između 500 i 1.000 osoba koje aktivno sudjeluju u tržištu bitcoina, najpoznatije svjetske kriptovalute. Primjetilo se da u posao s ovom elektronskom valutom ulaze i klasični ulagači, koje je privukao porast cijene bitcoina u kriznim vremenima. Pojedinačni bitcoin u jednom je trenutku bio dosegnuo čak i cijenu unce zlata, u četveroznamenkastim dolaskim iznosima. Danas se to promijenilo, pa se ovih dana na on-line burzama kretao između 370 i 390 dolara. Na početku cijena je bila preko 400 dolara, a nakon par mjeseci se kretao između 250 i 300 dolara. Ove poveće varijacije pokazuju da bitcoinom trguju uglavnom ulagači skloniji rizičnim ulaganjima, posljedično i većoj zaradi ukoliko pogode pravo vrijeme.

Bitcoini su korišteni i u Hrvatskoj kao sredstvo kriminalnog plaćanja. Jedno vrijeme je postojala organizirana skupina koja je hakirala računala i potom tražila novce, pod prijetnjom brisanja svih podataka. Kao sredstvo plaćanja tada su tražili bitcoine, najčešće u protuvrijednosti od tri do pet tisuća kuna. Danas se sve više bitcoini u Hrvatskoj kriste u klasične svrhe – kupnju dobara i usluga. Prema podacima dostupnima od tvrtke BSpend, koja najviše radi s bitcoinima

[27] http://www.poslovni.hr/hrvatska/prodaje-se-prva-kriptovila-u-hrvatskoj-345023?utm_source=Facebook&utm_medium=Status&utm_content=345023&utm_campaign=FB+page+status

u Hrvatskoj, već sada ima 20-ak mjesta u Hrvatskoj gdje se može plaćati bitcoinima. Zagreb nije grad s najviše takvih mjesta, ima ih četiri, dok je u Splitu pet. Split je zanimljiv i zbog još jedne stvari: dok u većini slučajeva mogućnost plaćanja bitcoinima omogućuju tvrtke iz domene turizma i IT-a, u Splitu je ovom kritpovalutom moguće platiti proizvode i u jednoj stolariji.[28]

Stranica LIDER navodi primjer Splitske IT tvrtke Avensys koja je uvela plaćanje proizvoda i usluga u kriptovalutama, a direktor Frane Cvitanić kaže da se na taj potez odlučio kako bi bio korak ispred konkurencije. Avensys je tako postao prva digitalna agencija u Splitu koja prihvaća kriptovalute kao način plaćanja. Klijenti na raspolaganju imaju plaćanje u raznim kriptovalutama poput bitcoina, ethera, ripplea, litecoina, dasha i mnogih drugih.
U početnom razdoblju plaćanje se odvijalo tako da se pola plaćalo u kriptovaluti, a pola konvencionalnom valutom. Imali su pregovore s prvim klijentom koji je odlučio plaćanje obaviti na taj način, nakon čega je Cvitanić rekao kako će možda uvesti 100-postotno plaćanje kriptovalutom, ovisno o dogovoru s klijentima.
Na domaćoj sceni postoje firme koje prihvaćaju plaćanje u kriptovalutama, međutim to još nisu javno objavile. Danas firme posluju u turbulentnoj okolini, došlo je do prezasićenosti gomilom podataka, a konkurencija i tržište su neumoljivi. Kriptovalute su sadašnjost i budućnost plaćanja, kaže Cvitanić. U računovodstvenom smislu kriptovaluta se ne može smatrati materijalnom imovinom jer svrha virtualne valute je da služi kao sredstvo plaćanja, dok istovremeno ne predstavlja vrijednosni papir, ističe Cvitanić koji s knjigovođama razmatra način bilježenja kriptovaluta u poslovnim knjigama jer RRiF još nije izdao smjernice o tome.[29]

4.3. Primjeri kako uložiti 100 $ u btc?

Potrebno je pronaći razmjenu koja prodaje Bitcoin u vašoj regiji, a zatim kupiti Bitcoin od 100 dolara. Nakon toga dobijete novčanik kao što je knjiga nano S. Preporučuje se hardverski novčanik jer omogućuje kontrolu novčića. Bitcoin je potrebno čuvati duže vremena (više od godinu dana), te se može izvući navedena investicija ili ih nastaviti držati.

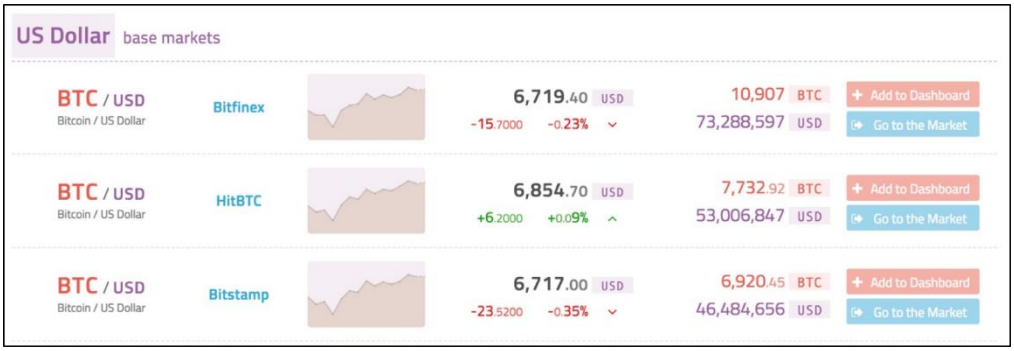
[28] http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Bitcoin-koristi-500-do-tisucu-Hrvata-njime-placaju-cak-i-stolariju
[29] https://lider.media/aktualno/tvrtke-i-trzista/poslovna-scena/tvrtka-avensys-uvela-je-placanje-u-kriptovalutama/

Nakon što se odobri kupnja (to može potrajati danima, satima ili samo nekoliko trenutaka), može se ići naprijed i kupiti za bitcoin 100 USD. Cijena će vjerojatno biti nešto više od toga jer većina brokera ili naplaćuje pristojbu ili skrivaju pristojbe u cijenu bitcoina. Brokeri koji pokazuju veću cijenu za bitcoin često skrivaju cijenu u cijenu. Potrebno je provjeriti nedavnu povijest cijena sa brokerom (tijekom posljednja 2-4 tjedna trebalo bi biti dovoljno).

Ako je bitcoin na novom visoku, oduprijeti se zahtjevu. Cijena je vjerojatno da će se "povući" uskoro prije (vjerojatno) ići gore. Ako je cijena nedavno pala, no od tada je stabilizirana ispod nedavne visoke razine, vjerojatno dobivate mnogo bolji posao i dobit ćete više bitcoina za svoj dolar kao nagradu za strpljenje i vrijeme.

Sada ste uložili u Bitcoin. Vjerojatno je da će vaš broker držati bitcoin za vas, prenijeti ga na privatni novčanik, potrošiti s nekim tko prihvaća Bitcoin za plaćanje ili učiniti sve što želite.

Također možete kupiti $ 100 u bitcoin od nekog drugog koji je spreman prodati vam svoj bitcoin u privatnoj prodaji, gdje vam dati novac i oni poslati bitcoin na svoj novčanik. Morat ćete unaprijed postaviti (oni su besplatni). [30]



Slika 7. Konverzija US dollar u Bitcoine

[30] https://www.investopedia.com/articles/investing/123015/if-you-had-purchased-100-bitcoins-2011.asp

5. ZAKLJUČAK

Prema zagovornicima kriptovaluta, digitalne valute imaju nekoliko glavnih obilježja koja se navode kao prednost i razlog za prihvaćanje njihove uporabe. Ova obilježja nalaze se na puno mjesta gdje se objašnjava definicija neke digitalne valute, kao na primjer Bitcoin-a, a to su prije svega:

- decentraliziranost
- ograničenost količine novčanih jedinica
- anonimnost korištenja
- praktičnost i efikasnost korištenja, pogotovo u internetskoj trgovini

Iz navedenog je vidljivo kako nove digitalne valute donose novu dimenziju u razmjeni vrijednosti i trgovini, u praktičnom smislu, boljom efikasnošću, novim mogućnostima, uštedama u vremenu i cijeni i slično, ovisno od primjene do primjene. U tom smislu, ova tehnologija je dobitak za društvo.

Jedno od najzanimljivije pitanja jest ono regulacije količine novca u opticaju. Iako je broj novčanih jedinica pojedine digitalne valute kontroliran i predvidljiv, često se zanemaruje da su digitalne valute u velikoj mjeri međusobni supstituti.

Sve već i broj korisnika digitalnih valuta, i sve veća pozornost javnosti prema njima u zadnje vrijeme, uzrokovana je najčešće velikim porastom tečaja/cijene svih digitalnih valuta na tržištu. Stvara se izuzetno primamljiva prilika za špekulativna ulaganja i ostvarivanje velikih prinosa. To se može lako isčitati iz kretanja tečaja/cijena prikazanih u zadnjem dijelu rada.

Neovisno u kojem smjeru će se stvari razvijati, činjenica je da digitalne valute istovremeno donose nove mogućnosti ali i nove nedostatke i probleme. Kao i mnogo puta ranije, nove tehnološke mogućnosti mogu se iskoristiti i u pozitivnom i u negativnom smislu što smo pokušali prikazati u prvom dijelu rada. Digitalne valute su novi ekonomski alat, čiji značaj, doprinos i korisnost ovise prije svega o okolnostima i načinu korištenja.

Navedeni primjeri u radu upravo to i pokazuju. Njihovo korištenje omogućava lakšu i bržu razmjenu, u pojedinim slučajevima i transparentniju ali trenutno, barem u Hrvatskoj ipak još slabo rasprostranjenu. Postoje naznake rasta korištenja kriptovaluta u Zapadnim zemljama u kojima je izražena informatička ali i ekonomska pismenost dok se u zemljama u razvoj, poput

Hrvatske, ipak taj rast nije tako visok. U Hrvatskoj se pokazuje potencijal za razvoj no, osim pojedinih entuzijasta i dalje je dug proces uvođenja u poslovanje kao sredstvo plaćanja

6. LITERATURA

1. Sajter, D., „Financijska analiza kriptovaluta u odnosu na standardne financijske instrumente“, Financije- teorija i suvremena pitanja, EFOS, 2017
2. CHENG, Cecilia, LI, Angel Yee-lam, Internet addiction prevalence and quality of (real) life: A metaanalysis of 31 nations across seven world regions, Cyberpsychology Behav. Soc. Netw., sv. 17, izd. 12, 2014, str. 755–760
3. MIRONOV, Ilya, OTHERS, Hash functions: Theory, attacks, and applications, Microsoft Res. Silicon Val. Campus Noviembre De, 2005, Dostupno na: http://www.engr.uconn.edu/~akiayias/cse281sp08/CSE281_Computer_Security/Reading_files/hash_survey.pdf.
4. BURR, William E., Selecting the advanced encryption standard, IEEE Secur. Priv., sv. 99, izd. 2, 2003, str.43–52
5. FAIRFIELD, Joshua AT, BitProperty, Cal Rev, sv. 88, 2014, str. 820
6. ALI, Robleh i ostali, The economics of digital currencies, 2014, str. 279
7. CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/
8. COINDESK, How can I buy bitcoins?, CoinDesk, 20-kol-2013, Dostupno na: http://www.coindesk.com/information/how-can-i-buy-bitcoins/.
9. Bitcoin ATM Map, Dostupno na: https://coinatmradar.com
10. BUKHARI, Jeff, Bitcoin: Winklevoss ETF May Not be Dead Yet, Fortune, Dostupno na: http://fortune.com/2017/03/23/why-the-winklevoss-bitcoin-etf-may-not-be-dead-yet/
11. https://crobitcoin.com/bitcoin/sto-je-bitcoin/
12. https://crobitcoin.com/altcoin/ethereum/
13. FAIRFIELD, Joshua AT, BitProperty, Cal Rev, sv. 88, 2014, str. 820

14. DOWD, Kevin, HUTCHINSON, Martin, Bitcoin will bite the dust, Cato J, sv. 35, 2015, str. 359,364
15. www.kriptovalute.hr
16. http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Bitcoin-koristi-500-do-tisucu-Hrvata-njime-placaju-cak-i-stolariju
17. https://lider.media/aktualno/tvrtke-i-trzista/poslovna-scena/tvrtka-avensys-uvela-je-placanje-u-kriptovalutama
18. https://www.investopedia.com/articles/investing/123015/if-you-had-purchased-100-bitcoins-2011.asp

7. SAŽETAK

U svijetu gdje tehnologija preuzima sve veću ulogu, gdje je područje bez interneta nemoguće zamisliti, a dobar dio ljudi uslijed financijskih kriza izgubio povjerenje u financijske sustave javila se potreba za drugačijim pristupom u rješavanju poteškoća. Kriptovalute su donijele cijeli niz drugačijih postavki financijskog sustava koji je u mnogočemu različit od tradicioalnih novčanih oblika. Zadnjih nekoliko godina digitalni novac općenito, a posebno nove digitalne valute sve više postaju predmet interesa javnosti. Velika praktičnost i brzina obavljanja elektroničkih transakcija u odnosu na klasične, su čimbenici koji već sada nedvojbeno utječu na porast popularnosti različitih oblika elektroničkog plaćanja. Digitalne valute na ovom polju donose nove mogućnosti uporabe. U svijetu postoji cijeli niz primjera plaćanja kriptovalutama i razmjena cijelih poslovnih procesa putem istih. U Hrvatskoj postoji još određena skepsa prema njihovom korištenju te je nogo manja mogućnost njihovog korištenja.

Ključne riječi: krptovalute, bitcoin, međunarodno poslovanje

8. SUMMARY

In a world where technology plays an increasingly important role, where the area without internet is impossible to imagine, and a good deal of people lost their trust in financial systems due to financial crises, there was a need for a different approach to dealing with issues. Chrysanthemums have brought a whole host of different financial system settings that are in many ways different from traditional financial forms. Over the past few years, digital money in general, and especially new digital currencies, has become increasingly the subject of public interest. The great convenience and speed of doing electronic transactions in comparison with the classical ones are factors that already undoubtedly affect the popularity of various forms of electronic payment. Digital currencies in this field bring new opportunities to use. In the world there is a whole range of crypt valued payments and the exchange of entire business processes through the same. There is still a certain disparity in Croatia in terms of their use, and there is a lesser possibility of their use.

Keywords: cryptovalute, bitcoin, international business

9. POPIS SLIKA I TABLICA